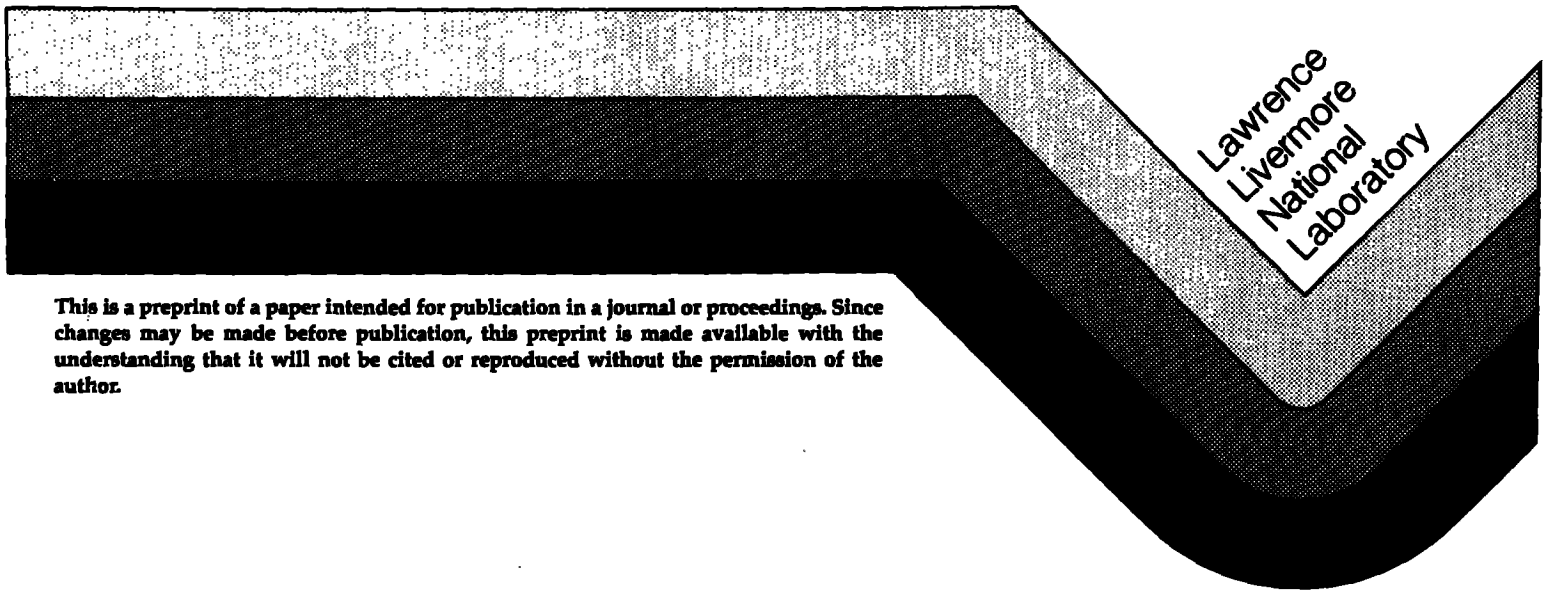
UCRL- 94320
PREPRINT

INSIDER PROTECTION -- A REPORT CARD

Rokaya A. Al-Ayat
Bruce R. Judd

This paper was prepared for submittal to
INMM 27th Annual Meeting
New Orleans, Louisiana
June 22-25, 1986



INSIDER PROTECTION -- A REPORT CARD

Rokaya A. Al-Ayat, and Bruce R. Judd

Lawrence Livermore National Laboratory*

Livermore, California

Abstract

Enhanced security measures against external threats (e.g., terrorists, criminals) have been implemented at most facilities that handle special nuclear material, classified information, or other assets critical to national security. Attention is now focussing on insider protection, and safeguards managers are attempting to provide balanced protection against insider and outsider threats. Potential insider threats include attempts by facility employees to steal special nuclear material (SNM), to cause a radiological hazard to the public, to sabotage critical facilities, or to steal property or classified information. This paper presents a report card on the status of insider protection at Department of Energy and Nuclear Regulatory Commission-licensed facilities, with emphasis on SNM theft. We discuss the general trends in insider protection and the limitations of protection measures currently in use. We also discuss the most critical needs for improved procedures, technology, analytical tools, and education for safeguards personnel.

Introduction

The increasing number of international terrorism incidents, espionage cases, and general public concerns have motivated a higher level of effort to protect facilities, materials, and information against a spectrum of potential threats. Highly visible upgrades to physical protection at Department of Energy (DOE) and Nuclear Regulatory Commission (NRC)-licensed facilities have substantially increased protection against "outsider" threats (e.g., terrorist or criminal adversaries). Attention is now focusing inward toward potential insider threats, especially employees who have routine access to nuclear materials, classified information, and critical facilities. As a result, safeguards managers must attempt to provide balanced protection against both insider and outsider threats.

During the past ten years Lawrence Livermore National Laboratory (LLNL) has been evaluating the effectiveness of insider protection at DOE and NRC facilities. This paper provides a report card on insider protection based on LLNL findings at many facilities that handle special nuclear material, classified information, and other critical assets. The report card does not address specific levels of protection or vulnerabilities, but rather it focuses on general trends and insights into current insider protection effectiveness and areas for improvement. In particular, we discuss the need for better understanding on the part of safeguards managers, improved protection technology and procedures, and easy-to-use evaluation tools that cover the full range of potential insider threats.

The paper comprises four sections. In the first, we identify the spectrum of potential insider threats and highlight difficulties in providing protection against them. In the second section, we discuss the general approaches to insider protection and briefly describe their limitations. In the third section, we introduce the types of analytical tools that are available to measure safeguards effectiveness, and in the fourth, we summarize improvements needed in protection measures and evaluation tools.

Potential Threats

Potential insider adversaries include anyone with access to safeguarded assets. Consider, for example, a facility that manufactures reactor fuel containing highly enriched uranium or plutonium. Potential adversaries include process operators and supervisors, nuclear material custodians and accountants, maintenance and health physics personnel, janitors, security inspectors, process engineers, plant managers, secretaries, computer programmers, and many others. The goals of the adversary could fall into any of five broad categories: threats to special nuclear material (SNM), radiological sabotage, industrial sabotage, theft of classified information, or theft of property. Threats to SNM include theft, diversion (removing the material from its authorized location but not removing it from the facility all

*Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

together), and falsification of accountability records to cover up a theft or to give the appearance of theft when, in fact, none has occurred (a form of sabotage).

Insider threats can be characterized as covert or overt and violent or non-violent. It is easy to conceive of scenarios where an adversary follows a covert, non-violent strategy until he or she is detected, in which case overt force might be used.

The primary difficulty in providing insider protection is that potential adversaries have routine access to the protected asset as well as knowledge of operations and safeguards. Thus, they may have the opportunity to steal the asset or damage it. Also, in contrast to terrorist-type attacks on DOE or NRC facilities (which have not occurred), insider-type events occur, ranging from daily property theft to infrequent but more consequential espionage. Finally, protection against such events almost always constrains productive activities and therefore can be very costly.

Protection Measures

Insider protection requires an integrated system of protection measures, including:

- Human reliability programs.
- Physical protection.
- Material control.
- Material accounting.

Human reliability programs (HRP), including security clearances, security awareness activities, and psychological screening programs are designed to reduce the likelihood of or deter malevolent acts. As with all protection measures, HRP activities have limitations and cannot be relied upon totally to eliminate potential insider threats. Moreover, an otherwise reliable insider may be coerced. Therefore, facilities must use physical protection, material control, and material accounting systems to detect or prevent attempts if the human reliability program fails.

Physical protection includes several measures, such as containment and access controls. These may limit access to the assets, but some insiders generally have the access or authority to override physical protection measures. In fact, physical protection in the form of armed security inspectors can exacerbate rather than reduce the potential insider threat.

Material control and accountability (MC&A) systems are mainstays of insider protection against SNM theft. However, these systems rely heavily on administrative procedures that can be circumvented if not designed properly. MC&A systems also rely on hardware such as SNM monitors in doorways or periodic physical inventories, both of which may be subject to tampering or inaccurate measurements. Furthermore, material accounting systems can be subject to inadvertent errors or to falsification, which decreases confidence in them.

Whereas protection against SNM theft has been strengthened, better methods of protecting against sabotage, compromise of classified information, and property theft are needed. For example, there is no equivalent to the portal SNM monitor for classified documents; explosives detection is an inexact science, and property theft is an increasing and universal problem.

Overall, insider protection is a "tough course," and many systems receive no more than a passing grade. On the brighter side, insider protection at many facilities is improving and funding for safeguards upgrades is increasing. Further, the options for improving protection against insiders cost less than upgrades to outsider protection.

Effectiveness Evaluation

The first step toward improving insider protection is evaluating the effectiveness of existing safeguards. For threats related to SNM theft, there are several systematic and quantitative methods for evaluating safeguards effectiveness, though they have limitations. Some methods are detailed -- designed to evaluate the effectiveness of safeguards when confronted with every conceivable adversary action. Others are aggregated: they provide a "first cut" evaluation to identify weaknesses and to determine where detailed analysis is warranted. Such methods are available through national laboratories, consulting companies, and some DOE contractors and NRC licensees.

For other threats, there are fewer systematic evaluation approaches. Systematic approaches have been developed to help identify vulnerabilities to radiological sabotage, and, in some cases, industrial sabotage. These methods are gaining acceptance by facility managers. Also, systematic methods for evaluating computer security systems are becoming more readily available, but these methods are not yet used widely. Such formal methods are not available for the general classified information problem, in spite of the fact that at many research facilities, protecting classified information poses a challenge similar to protecting SNM.

Despite the lack of formal tools for analyzing some threats such as classified information, decisions are being made on allocating budgets to maintain or enhance overall insider or insider/outsider protection. Such decision-making requires systematic methods for evaluating effectiveness against all threats. In addition, decision makers could improve their use of safeguards resources if they had an analytical tool for combining considerations of all threats and allocating limited resources to achieve maximum risk-reduction at minimum cost.

Needed Improvements

Several improvements are needed to enhance insider protection. These are in the areas of education, procedures, technology, and analytical tools.

Facility safeguards personnel need a better understanding of the nature of the insider threat, the limitations of available protection measures, and training in how to apply appropriate evaluation methods. Increased awareness can make a significant difference in protection levels with minimal cost or operational impact.

Improperly implemented procedures are the most frequently encountered weaknesses in insider protection systems. If those who design, train, supervise, and evaluate procedures simply adopt a "black hat" approach and answer the question "How can an adversary circumvent these procedures?," then many vulnerabilities can be avoided.

Technology can help, and improvements should be pursued. For example, SNM portal monitors in use throughout the industry only detect the presence of material, but not the quantity. Reliable instruments to provide a rough estimate of the quantity would significantly improve material control through portals. Better access controls and methods for "compartmenting" facilities are needed to limit further the number of insiders with access to safeguarded assets.

Enhanced technology could also improve material accounting systems. Facilities that process bulk material depend heavily on periodic measurements and material balances to ensure that all materials are accounted for. In some cases, excessive inventory differences can be reduced by improving the choice of measurement points and measurement technology. This may also help eliminate the long-standing problem of resolving the cause of inventory differences and may help a facility identify more rapidly whether an indication of missing material is an error or an actual loss.

Care must be taken when technological solutions are attempted. For example, most facilities now have computerized nuclear material accounting systems. In some cases, double-entry manual systems have been replaced by single-entry computerized accounting packages. While this may increase the efficiency of data entry, it may eliminate redundant safeguards and may reduce the likelihood of catching data entry errors.

In addition to technological improvements, additional new analytical tools and improvements to existing tools are needed. For example, while there are aggregated and detailed approaches for evaluating protection of SNM, these cover only some of the protection measures. Better methods are needed for evaluating the effectiveness of material accounting systems in detecting losses after-the-fact and for comparing that effectiveness to the timely detection capabilities of physical protection and material control. Another useful tool would evaluate human reliability programs in common terms with physical protection, material control, and material accounting safeguards. This evaluation would allow safeguards managers to make tradeoffs between improvements in HRP to deter malevolent acts versus other safeguards to prevent their success if deterrence fails.

As mentioned in the previous section, new analytical approaches are needed for evaluating safeguards effectiveness against theft of classified information. Also, decision makers need a method for combining the total spectrum of potential threats and allocating resources cost-effectively.

In addition, more training is needed for facility safeguards analysts, so they can apply the tools themselves, rather than relying on others. This means that the tools must be designed for use in-house: they must be readily available and easy to use.

Facility safeguards managers also need methods to validate the effectiveness of their insider protection systems. Whereas analytical tools make quantitative estimates of effectiveness levels, one of the best ways to increase the confidence in protection systems is to test them in realistic situations. More frequent use of the "insider equivalent" of force-on-force exercises could substantially increase confidence in insider protection and, at the same time, improve the training and awareness of safeguards personnel.

In summary, insider protection is improving, but there are several areas where more work is needed. Perhaps the greatest need is to build in-house safeguards evaluation capabilities. This should be accompanied by better procedures, technology, and analytical tools for safeguards designers and managers.